APRIL — 23 — 2014 | VOLUME 03. ISSUE 02

CS BITS & BYTES

HIGHLIGHTING INNOVATIVE COMPUTER SCIENCE RESEARCH

Quantum leap in computing

Quantum computers could perform more calculations at faster speeds than classical computers

ABOVE IMAGE

Video from NBC Learn at https://www.nbclearn.com/sciencenews/cuecard/63282.

“So the million dollar question is, can these quantum computers actually be built?”

SCOTT AARONSON
MIT

Every year, cellphones, laptops, and other computing devices get smaller and faster. It might seem like — with enough elbow grease — scientists and engineers could keep making computers smaller and faster.

However, computers as we know them – **classical computers** – have certain fundamental limitations to their size and speed. For instance, there are extremely complex problems that would take classical computers so long to solve that their answers would be essentially useless.

To find ways around the limitations of classical computers, scientists are working to design a totally different kind of computer, called a **quantum computer**. In theory, quantum computers could perform computations that use the unusual physical properties of very small things like atoms or photons.

With classical computers, a transistor is used to transmit a single **bit** of information. When the bit is a “1,” the transistor is on and when the bit is a “0,” the transistor is off. Series of bits encode information and actions for the computer.

However, the basic principle underlying quantum computers is that they will use quantum bits, called **qubits** (pronounced ‘kyoobit), which can exist simultaneously as 1 and 0.

The incredible power of quantum computers stems from the fact that materials making up the qubits communicate and react simultaneously when one qubit is manipulated – behaving like a single coherent system. This would enable quantum computers to perform far more calculations at one time than classical computers – if they could be built.

Scientists theorize that they can make qubits for quantum computers out of a number of different physical systems — from lasers, to ultra-cold atoms, to complex molecules. Yet, quantum computers are easier to think about than to build in real life. If we can make quantum computers, scientists hope to use them to protect information, predict the future climate and perform other superfast calculations. **What would you do with a quantum computer?**

Who does this stuff?

Scott Aaronson is a theoretical computer scientist and an associate professor of Electrical Engineering and Computer Science at Massachusetts Institute of Technology (MIT). Dr. Aaronson is a leading scholar in the capabilities and limits of quantum computers and computational complexity theory more generally. He received a G.E.D. from New York State, graduated from Cornell University, and earned his Ph.D. in Computer Science from the University of California, Berkeley. Dr. Aaronson has written extensively about quantum computation, including through a popular blog at http://www.scottaaronson.com/blog.

SCOTT AARONSON

TRY THIS OUT

CS BITS & BYTES

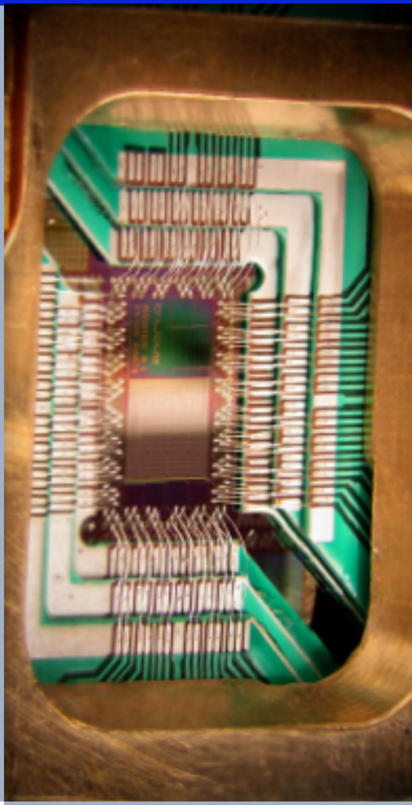
One famous example of a very hard problem for classical computer involves semiprimes—numbers that are the product of two primes. If you give a classical computer a large semiprime (for example 8,166,877), it will take the computer a very long time to figure out that it has two prime factors (3571 and 2287). As you make the size of the semiprime only a few digits longer, the time it takes for a classical computer to find the prime factors increases exponentially. This kind of factoring is so hard we use it as the basis for public key cryptography, a secret code to help people communicate private digital information.

1. Form a few teams of individuals, each with some basic calculators with simple addition, subtracting, multiplication and division capabilities. (Or, if you want to hone their arithmetic skills, have them do this without calculators!)

2. Using the list of primes at http://primes.utm.edu/lists/small/10000.txt generate a small semiprime using two 1 digit primes. Give this to each team and see which one factors it first.

   A. Repeat with two primes, each with 2 digits.

   B. Repeat again with two primes with 3 digits.



Photograph of a chip constructed by D-Wave Systems Inc. designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor, mounted in a sample holder. Credit: D-Wave Systems, Inc.

Learn More

Video from NBC Learn

https://www.nbclearn.com/sciencenews/cuecard/63282

Scott Aaronson

http://www.scottaaronson.com/

Aaronson on "Is There Anything Beyond Quantum Computing?"

http://www.pbs.org/wgbh/nova/blogs/physics/2014/04/is-there-anything-beyond-quantum-computing/

Quantum-computer company D-Wave Systems

http://www.dwavesys.com/quantum-computing

More on the limitations of computing from *CS Bits & Bytes*

http://nsf.gov/cise/csbytes/newsletter/vol2/vol2i14.html

ABOUT

CS Bits & Bytes is a bi-weekly newsletter highlighting innovative computer science research. It is our hope that you will use CS Bits & Bytes to engage in the multi-faceted world of computer science to become not just a user, but also a creator of technology. Please visit our website at: www.nsf.gov/cise/csbytes.